**Information Governance Breach Reporting Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| 1.1 | June 2022 |  | AJH |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table of contents**

[1 Introduction 3](#_Toc98154408)

[1.1 Policy statement 3](#_Toc98154409)

[1.2 Status 3](#_Toc98154410)

[1.3 KLOE (England only) 3](#_Toc98154411)

[1.4 Training and support 4](#_Toc98154412)

[2 Scope 5](#_Toc98154413)

[2.1 Who it applies to 5](#_Toc98154414)

[2.2 Why and how it applies to them 5](#_Toc98154415)

[3 Managing incidents 5](#_Toc98154416)

[3.1 Overview 5](#_Toc98154417)

[3.2 UK GDPR reporting requirements 5](#_Toc98154418)

[3.3 Breach of patient confidentiality 6](#_Toc98154419)

[3.4 Incorrect disposal of confidential material 6](#_Toc98154420)

[3.5 Computer misuse by an authorised user 7](#_Toc98154421)

[3.6 Attempted/actual theft and/or access by an unauthorised person 8](#_Toc98154422)

[3.7 Lost or misfiled paper medical records 9](#_Toc98154423)

[4 Reporting incidents and processes 10](#_Toc98154424)

[4.1 Internal process 10](#_Toc98154425)

[4.2 External process 10](#_Toc98154426)

[4.3 Lessons learned 10](#_Toc98154427)

[4.4 When do individuals have to be notified? 10](#_Toc98154428)

[5 Legal framework 11](#_Toc98154429)

[6 Training 12](#_Toc98154430)

# Introduction

## Policy statement

This document sets out how Grey Road Surgery will investigate and manage information incidents and provide organisational staff with guidelines to identify and report information incidents including near misses.

Where relevant this should be read in conjunction with the [Business Continuity Plan](https://practiceindex.co.uk/gp/forum/resources/business-continuity-policy.1056/), the [UK General Data Protection Regulation](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) (GDPR) and the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) which introduce new requirements for breach reporting.

The procedures apply to incidents that impact on the security and confidentiality of personal information. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than simply losing personal data.

These information incidents can be categorised by their effect on patients and their information:

* **Confidentiality** e.g., unauthorised access, data loss or theft causing an actual or potential breach of confidentiality
* **Integrity** e.g., records have been altered without authorisation and are therefore no longer a reliable source of information
* **Availability** e.g., records are missing, mis-filed or have been stolen, compromising or delaying patient care.

## Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](https://www.gov.uk/guidance/equality-act-2010-guidance). Consideration has been given to the impact this policy might have with regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

## KLOE (England only)

The Care Quality Commission would expect any primary care organisation to have a policy to support this process and this should be used as evidence of compliance against CQC Key Lines of Enquiry (KLOE).

Specifically, Grey Road Surgery will need to answer CQC key questions on “Safe,” “Effective” and “Well-led.”

The following is the CQC definition of Safe:

*“By safe, we mean people are protected from abuse\* and avoidable harm. \*Abuse can be physical, sexual, mental, or psychological, financial, neglect, institutional or discriminatory abuse.”*

|  |  |
| --- | --- |
| **CQC KLOE S6** | Are lessons learned and improvements made when things go wrong? |

The following is the CQC definition of Effective:

*“By effective, we mean people’s care, treatment and support achieves good outcomes, promotes a good quality of life and is based on the best available evidence.”*

|  |  |
| --- | --- |
| **CQC KLOE E3** | How does the service make sure that staff have the skills, knowledge, and experience to deliver effective care, support, and treatment? |

The following is the CQC definition of Well-led

*“By well-led, we mean that the leadership, management, and governance of the organisation assures the delivery of high-quality and person-centred care, supports learning and innovation, and promotes an open and fair culture.”*

|  |  |
| --- | --- |
| **CQC KLOE W4** | Are there clear responsibilities, roles and systems of accountability to support good governance and management? |
| **CQC KLOE W5** | Are there clear and effective processes for managing risks, issues, and performance? |
| **CQC KLOE W8** | Are there robust systems and processes for learning, continuous improvement and innovation? |

## Training and support

Grey Road Surgery will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

# Scope

## Who it applies to

This document applies to all employees, partners and directors of the organisation. Other individuals performing functions in relation to the organisation such as agency workers, locums and contractors are encouraged to use it.

Furthermore, it also applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS).[[1]](#footnote-1)

## Why and how it applies to them

All staff at Grey Road Surgery are to be fully conversant with this policy and are to understand the requirement for reporting breaches in information governance.

# Managing incidents

* 1. **Overview**

The Senior Information Risk Owner (SIRO) will assign the role of incident manager (delegated authority) who in conjunction with the Data Protection Officer (Art 37 UK GDPR) will assess and manage all UK GDPR/Information Governance and Data Protection breaches.

The organisation’s Data Protection Officer (DPO) is IM Merseyside Governance Team

Any actual or potential information incident in the organisation will be assigned to one of the following categories below (the list is not exhaustive) and investigated and managed accordingly.

The DPO will, using the [Guide to the Notification of Data Security and Protection Incidents](https://www.dsptoolkit.nhs.uk/Help/Attachment/148), grade the breach and provide appropriate advice with regard to reporting and the management of the breach.

* 1. **UK GDPR reporting requirements**

The UK GDPR introduced a duty on all organisations to report certain types of data breach to the relevant supervisory authority and in some cases to the individuals affected (Art 33).

Grey Road Surgery must notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

The above must be assessed on a case-by-case basis by the organisation’s DPO and SIRO/Caldicott Guardian. Therefore, a breach MUST be reported to the Information Governance Lead, DPO and SIRO/Caldicott Guardian within 24 hours of the organisation becoming aware of it so that an appropriate assessment can take place.

* 1. **Breach of patient confidentiality**

Grey Road Surgery will:

* Interview the complainant to establish the reason for the complaint and why the organisation is being considered responsible
* Investigate according to the information given by the complainant
* Ensure the investigator records the findings within the reporting system, e.g., unsubstantiated concern, suspected/potential breach, actual breach, etc.
* Where necessary, provide a written explanation to the complainant with a formal apology if warranted
* Take and document appropriate action, e.g., no further action as there is no evidence that information was put at risk, advice/training, disciplinary measures, etc.
* Report the breach to the supervisory authority (the Office of the Information Commissioner) via the DSP Toolkit within 72 hours of being aware of the breach and undertake any recommendations as suggested following the reporting procedure
	1. **Incorrect disposal of confidential material**

This type of incident may lead to a breach of confidentiality and is likely to be reported by a patient affected, a member of the public or a member of staff and could be paper, hard drive, disks/tapes, etc.

Grey Road Surgery will:

* Investigate how the information left the organisation by interviewing staff and contractors as appropriate
* Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g., breach of confidentiality, misuse of data
* Consider whether the patient(s) should be informed and where it is judged necessary, provide a written explanation to the patient(s) with a formal apology
* Ensure the investigator records the findings within the reporting system, e.g., potential breach, actual breach, evidence of misuse, etc.
* Take and document appropriate action, e.g., advice/training, disciplinary or contractual measures, etc.
* Report the breach to the supervisory authority (the Office of the Information Commissioner) via the DSP Toolkit within 72 hours of being aware of the breach and undertake any recommendations as suggested following the reporting procedure
	1. **Computer misuse by an authorised user**

This includes browsing medical records when there is no requirement to do so, accessing unauthorised internet sites, excessive/unauthorised personal use, tampering with files, etc.

Grey Road Surgery will:

* Interview the person reporting the incident to establish the cause for concern
* Establish the facts by asking the system administrator to conduct an audit on activities by the user concerned
* Establish whether there is a justified reason for the alleged computer misuse
* Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g., breach of confidentiality, the risk information may have been tampered with and consider whether the patient(s) should be informed
* Ensure the investigator records the findings within the reporting system, e.g., breach of confidentiality, evidence of tampering, fraud, carrying on a business, accessing pornography, etc.
* Take and document appropriate action, e.g., no action as allegation unfounded, training/advice, disciplinary measures, etc.
* Report the breach to the supervisory authority (the Office of the Information Commissioner) via the DSP Toolkit within 72 hours of being aware of the breach and undertake any recommendations as suggested following the reporting procedure
	1. **Attempted/actual theft and/or access by an unauthorised person**

This type of incident may lead to a breach of confidentiality, the risk that information has been tampered with or information not being available when needed.

Grey Road Surgery will:

* Check the hardware asset register to find out whether equipment is missing
* Investigate whether there has been a legitimate reason for the removal of the equipment (such as repair or working away from the usual base)
* If the cause is external, inform the police asking them to investigate and keeping them updated with the organisation’s findings
* Interview staff and check the data asset register to establish what data was being held and how sensitive it is
* Establish the reason for the theft/unauthorised access, such as:
* Items to sell
* Access to material to embarrass the organisation
* Access to material to threaten patients (blackmail, stigmatisation).
* Consider whether there is a future threat to system security
* Inform insurers
* Review the physical security of the organisation
* If there has been unauthorised access to the organisation’s computer system:
* Ask the system administrator to conduct an audit to determine whether unauthorised changes have been made to patient records
* Consider whether any care has been provided to patients whose records have been tampered with
* Check compliance with access control procedures, e.g., ensure passwords have not been written down, staff members are logging out properly, etc.
* Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate (e.g., warning patients)
* If computer hardware or the core software has been stolen, inform the system administrators/suppliers to enable the restoration of system data to new equipment
* Ensure the investigator records the findings in the reporting system, e.g., potential breach, actual breach, evidence of tampering, compromised or delayed patient care, etc.
* Take and document appropriate action, e.g., physical security improvements, advice/training, disciplinary measures, etc.
* Report the breach to the supervisory authority (the Office of the Information Commissioner) via the DSP Toolkit within 72 hours of being aware of the breach and undertake any recommendations as suggested following the reporting procedure
	1. **Lost or misfiled paper medical records**

This type of incident could have a severe impact on patient care as the information within a patient’s record may be incorrect or not available when required.

Grey Road Surgery will:

* Investigate who last used/had the paper record by interviewing staff and contractors as appropriate
* Consider whether any care has been provided based on incorrect information within a patient record
* Consider whether patient care has been delayed due to information not being available
* Establish whether the missing information can be reconstituted, e.g., from electronic records
* If information within records has been mis-filed, ensure it is restored to the correct filing order/returned to the correct record
* Where necessary, (i.e., if care is affected) provide a written explanation to the patient with formal apology
* Ensure the investigator records the findings in the reporting system, e.g., compromised or delayed patient care, etc.
* Take and document appropriate action, e.g., advice/training, disciplinary or contractual measures, etc.
* Report the breach to the supervisory authority (the Office of the Information Commissioner) via the DSP Toolkit within 72 hours of being aware of the breach and undertake any recommendations as suggested following the reporting procedure

# Reporting incidents and processes

* 1. **Internal process**

Incidents should be reported using the appropriate form and added to the Information Governance Incident Register and the DSP Toolkit.

The Information Governance Lead, SIRO/Caldicott Guardian and DPO must be informed within 24 hours of the incident being identified.

* 1. **External process**

Article 33 of the UK GDPR requires that a notifiable breach must be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it in accordance with the DSP Toolkit Handbook.

The UK GDPR recognises that it will often be impossible to investigate a breach fully within that time period and allows the organisation to provide information in phases.

Serious information incidents, i.e., those categorised as level 2 to 5 are to be reported to NHS England, the Clinical Commissioning Group and the Information Commissioner. Grey Road Surgery’s SIRO/Caldicott Guardian and DPO will notify the appropriate authorities.

* 1. **Lessons learned**

All registered incidents are re-evaluated after a six month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those types of incidents has reduced. If there is no change in the volume of each type of incident, the management team is alerted and appropriate action taken.

To provide staff with an example of what could occur, how to respond to such events and how to avoid them, previous incidents are used in security and confidentiality training sessions.

* 1. **When do individuals have to be notified?**

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be notified directly. A ‘high risk’ means the threshold for notifying individuals is higher than for notifying the relevant authorities as above, the organisation should also consider duties of candour.

The CQC document titled [The duty of candour: guidance for providers](https://www.cqc.org.uk/sites/default/files/20210421%20The%20duty%20of%20candour%20-%20guidance%20for%20providers.pdf) explains the requirements in detail including providing supporting examples for the different areas of healthcare provision and alludes to [Regulation 20: Duty of Candour](https://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-20-duty-candour) that provides the legal basis that relates to this subject.

Both the statutory duty of candour and the professional duty of candour have similar aims. These are to make sure that those providing care are open and transparent with the people using their services whether or not something has gone wrong.

The SIRO/Caldicott Guardian, with the DPO, will make the assessment about informing individuals of any breaches.

The Francis Inquiry Report indicated the importance of affected parties receiving a sincere apology for the impact that any incident can have on the patient, their families, next of kin and their carers especially in incidents that cause severe harm or the loss of life. A meaningful apology for the incident or the circumstances that have led to the incident is an important part of coping with the effect that it has caused and will demonstrate that the organisation has taken events seriously, be they major or minor.

The CQC guidance for providers states that saying sorry is not admitting fault, nor any admission of liability, but it is a crucial part of our duty of candour. To fulfil the duty of candour, this organisation will apologise for the harm caused, regardless of fault, as well as being open and transparent about what has happened.

An apology under the duty of candour does not constitute an admission of liability. Patients and relatives are to be offered detailed explanations of what led to the incident(s) occurring and their outcomes as well as a sincere apology and an acknowledgement of the impact it has had on them. This helps them to understand that there are lessons that the organisation can learn to ensure this does not happen again in the future.

Further detailed information is available within the [Duty of Candour Policy](https://practiceindex.co.uk/gp/forum/resources/duty-of-candour-policy.816/)

# Legal framework

Grey Road Surgery staff have a legal duty to comply with the following guidance which gives the circumstances under which confidential information can be disclosed:

* [The Data Protection Act (2018)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiwg-PH5fz1AhUxQkEAHRX2DjwQFnoECA4QAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2018%2F12%2Fcontents%2Fenacted&usg=AOvVaw1nLdFiC3yrsnW5qE79iLDw)
* [The Computer Misuse Act (1990)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjtkovS5fz1AhVhoFwKHSnsCNkQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1990%2F18%2Fcontents&usg=AOvVaw1hrd6GOQftKy7ghGPjb-VU)
* [The Health and Safety at Work Act (1974)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiE1ofa5fz1AhWPa8AKHVctAnsQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1974%2F37%2Fcontents&usg=AOvVaw14VUyTl0-uN6DNmcZ_xe4m)
* [Human Rights Act (1998)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi2_e_i5fz1AhWVnVwKHcwmCaAQFnoECAwQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F1998%2F42%2Fcontents&usg=AOvVaw1e5pKwsX2UgNYm4kE-Im1z)
* [Regulation of Investigatory Powers Act (2000)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiVosLr5fz1AhUNO8AKHc1sBtUQFnoECAkQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2000%2F23%2Fcontents&usg=AOvVaw34iK5TZfl3M_XLHn7aKzSx)
* [Freedom of Information Act (2000)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiv7Znz5fz1AhWSYMAKHXPPCWkQFnoECBAQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fukpga%2F2000%2F36%2Fcontents&usg=AOvVaw2ED-_lceYVKNX9EF_BgWVI)
* [Health and Social Care Act (2008)](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjB2MD75fz1AhUXgFwKHW0hDukQFnoECBAQAQ&url=https%3A%2F%2Fwww.legislation.gov.uk%2Fid%2Fukpga%2F2008%2F14&usg=AOvVaw23UpPn3SpiJpcDTjYuIrUY)
* [The Caldicott Principles](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj03PmE5vz1AhWIiVwKHUbMCFQQFnoECA0QAQ&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fthe-caldicott-principles&usg=AOvVaw22orCuz9f5J5jLudjT1oIJ)
* [Confidentiality: NHS Code of Practice](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjw2_aT5vz1AhWGQkEAHbWpAcgQFnoECAwQAQ&url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fconfidentiality-nhs-code-of-practice&usg=AOvVaw2hk75WSFduGdzUEdh-Ntem)

# Training

Grey Road Surgery must ensure that all staff undertake appropriate information governance and UK GDPR training during induction and all existing staff must receive annual update training.

Further detailed information is available within the organisation’s Information Governance Training Policy.

#

1. [Network DES Specification](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjW_Mmq0vz1AhXCQEEAHXOHBpoQFnoECA4QAQ&url=https%3A%2F%2Fwww.england.nhs.uk%2Fpublication%2Fnetwork-contract-des-specification-2021-22%2F&usg=AOvVaw3xuhgNvg7oYsvX-M1E-Pns) [↑](#footnote-ref-1)